IN THE SPECIFICATION

At page 2, line 10 replace the paragraph as follows.

A typical wired LAN 12 includes a plurality of wired devices 16A-D, e.g., desktop personal computers (PCs), connected to the same or different sub-networks (subnets) , e.g., 18, 20, and 22 terminating at a router (not shown). The wired devices 16A-D are physically connected to each other through cabling (not shown) on the wired LAN 12. For example, PCs 16A and 16B are connected to subnet 18 while PCs 16C and 16D are connected to subnet 20. Subnets 18 and 20 are coupled to each other and to inner firewall router 24 via subnet 22. The inner and outer firewall routers 24 and 28 provide an authorization mechanism that assures only specified operators or applications can gain access to the wired LAN 12. The inner firewall router 24 links the wired LAN 12 to remote users seeking access through the wireless LAN 14 and the Internet 30. The outer firewall 28 limits access to the Virtual Private Network (VPN) server 26 by remote users seeking access through the Internet 30.

A1

At page 3, line 12, replace the paragraph as follows.

To maximize security and prevent unauthorized access to the wired LAN 12 from a rogue wireless device or AP, the wireless LAN 14 is isolated from the wired LAN 12. Put differently, the cabling that physically connects one wired device to another on the wired LAN 12 is different from the cabling ~~36~~ that connects one AP to another on the wireless LAN 14. Isolating the wireless LAN 14 from the wired LAN 12 prevents a wireless device from accessing a wired LAN 12 unless authorized to do so by the VPN server 26 and the inner firewall router 24. However, isolating the wireless LAN 14 from the wired LAN 12 is costly and labor intensive. Moreover, routing the wireless and other remote user traffic through the single VPN server 26 slows access for both, particularly if large files are being transferred. As the VPN server 26 and the firewalls 24 and 28 are busy checking or re-routing data communications packets, they do not flow through the network 10 as efficiently as they would if the VPN server 26 and the firewalls 24 and 28 were not in place. Additionally, if the VPN server 26 fails, wired network 12 access through the VPN server 26 is prevented for both wireless operators and remote users.

A2